



UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

United States of America

v.

ROMAN GRIDJUSKO

Case No. 17-931-M

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of Nov. 21-23, 2016 in the county of Chester County in the
Eastern District of Pennsylvania, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 1344	Bank Fraud
18 U.S.C. § 1029(a)(1)	Access Device Fraud
18 U.S.C. § 1028A	Aggravated Identity Theft

This criminal complaint is based on these facts:

See attached affidavit.

☒ Continued on the attached sheet.

Complainant's signature

Jonathan D. Speck, U.S. Postal Inspector

Printed name and title

Sworn to before me and signed in my presence.

Date:

July 10, 2017

City and state:

Philadelphia, Pennsylvania

Judge's signature

DAVID STRAWNBRIDGE

Printed name and title

USMS

AFFIDAVIT

I, Jonathan D. Speck, being duly sworn, do hereby state as follows:

1. I am employed as a U.S. Postal Inspector with the U.S. Postal Inspection Service, Wilmington, Delaware Domicile, and am authorized to conduct criminal investigations of violations of Title 18 of the United States Code. I am a case agent involved in the investigation of ROMAN GRIDJUSKO. I have been employed as a U.S. Postal Inspector since September 2005. I am currently assigned to the South Jersey Multi-Functional Team, which investigates violations of federal law, including identity theft, mail theft, access device fraud, wire fraud and mail fraud, among other offenses. Prior to this assignment, I was assigned to External Crime team assignments in both Baltimore, MD (from May 2010 – February 2015) and Charleston, WV (from September 2005 – May 2010). My education and training has included twelve weeks of Basic Inspector Training (BIT) at the Inspection Service's training academy in Potomac, MD, a federally-accredited law enforcement academy. The training covered various aspects of federal law enforcement, including the investigation of identity theft, credit card fraud, and other financial crimes. I have received instruction on conducting investigations of, and have in fact participated in investigations involving, identity theft and access device fraud offenses. Prior to entering the Inspection Service, I was employed as a State Trooper with the Maryland State Police for approximately eight years, after graduating from the Maryland State Police academy. After two years of working patrol duties as a uniformed State Trooper, I was reassigned to a Major Crime Unit where I investigated felony offenses as a criminal investigator, specializing in the investigation of identity theft and other financial crimes.

2. This affidavit is submitted in support of a criminal complaint and warrant to arrest GRIDJUSKO because there is probable cause to believe that GRIDJUSKO obtained stolen debit/bank card information, which was encoded (or re-encoded) onto magnetic-stripe cards (i.e., access devices). There is also probable cause to believe that GRIDJUSKO obtained stolen debit/bank card PINs (a means of identification) which corresponded to the stolen debit/bank card information in his possession. There is also probable cause to believe that GRIDJUSKO used that stolen debit/bank card information, along with the stolen debit/bank card PIN numbers, to withdraw money at ATMs by accessing bank customer accounts, over interstate wires, without authorization. There is also probable cause to believe that money orders were deposited into GRIDJUSKO's own Wells Fargo account, which had been fraudulently purchased using stolen debit/bank card information and corresponding stolen debit/bank card PIN numbers.

3. Accordingly, there is probable cause to believe that GRIDJUSKO committed bank fraud (18 U.S.C. § 1344), access device fraud (18 U.S.C. § 1029(a)(1)), and aggravated identity theft (18 U.S.C. § 1028A).

4. Through my training, experience, and discussions with other criminal investigators, generally during a "credit card skimming" scheme, a thief uses a small, hidden "skimmer" device to steal credit or debit/bank card information during otherwise legitimate credit or debit/bank card transactions. The thief will install the skimmer over (or interface with) the card-swipe mechanism on ATMs, gas stations, and other terminals. When a victim swipes her credit or debit/bank card, the skimmer captures the information stored in the card's magnetic

stripe. For debit/bank cards, the thief will often also capture personal identification number (“PIN”) information. This can be done a number of ways, including via a separate device installed on (or interfaced with) the keypad, via a camera installed nearby which records victims entering their PINs on the keypad. The thief will then retrieve the stolen data and use that data to make fraudulent charges either online or in person while using a counterfeit credit or debit/bank card, which will have the stolen data encoded (i.e., cloned) onto the counterfeit card’s magnetic stripe. In terms of the counterfeit card, sometimes the thief will use a newly manufactured counterfeit card, or reuse/re-encoded/re-purpose a card, like a gift card. If the skimmed information on the counterfeit card came from a debit/bank card and is married with a corresponding (stolen) PIN, the thief will often either withdraw cash from the victim-cardholder’s bank account or purchase money orders, which debits the victim-cardholder’s bank account. This is sometimes referred to as the “cash-out” portion of a credit card skimming scheme.

FACTS

I. In September 2016, Gridjuskö entered the U.S., opened a bank account, and began renting vehicles

5. According to Department of Homeland Security (“DHS”) records, on September 14, 2016, GRIDJUSKO, a citizen of Estonia, entered the United States on a tourist visa.

6. On September 15, 2016, GRIDJUSKO opened a checking account at a Wells Fargo in East Norriton, Pennsylvania in his own name, with an account number of xxxxxx4625 and associated debit card number of xxxx-xxxx-xxxx-1498. ATM video surveillance photos from September through December 2016, demonstrate GRIDJUSKO used this Wells Fargo account.¹

7. Rental records reflect that from September through December 2016, GRIDJUSKO rented vehicles on at least fourteen separate occasions. For most of those rentals, GRIDJUSKO provided an address of 9843 Wistaria Street, Philadelphia, Pennsylvania.

8. Through my training, experience, and discussions with other criminal investigators, those who engage in a credit card skimming scheme often use bank accounts to move proceeds of the crime and often use rental vehicles to help avoid detection by law enforcement.

¹ DHS records suggest GRIDJUSKO was outside the U.S. for most of October 2016, and activity occurred on this Wells Fargo account during that time from within the U.S. However, GRIDJUSKO used this Wells Fargo account after his return to the U.S. in October 2016, and GRIDJUSKO had an associated Wells Fargo debit card (last four digits of 1498) upon his arrest on December 9, 2016. In addition, through my training, experience, and discussions with other criminal investigators, those who engage in a credit card skimming scheme generally work with other persons to accomplish their fraud due to the complexity of these schemes. In the course of a credit card skimming scheme, multiple people could have access to a bank account which is otherwise in a sole person’s name.

II. In September 2016, USPS money orders were deposited into Gridjusko's Wells Fargo account which were fraudulently purchased using WSFS Bank customer accounts likely stolen/skimmed at Sainath Food & Fuel in Newark, Delaware

9. In September 2016, certain WSFS Bank customers reported that unauthorized/fraudulent debit card transactions had occurred on their respective accounts from between September 13–14, 2016. Most, if not all, of the cardholders still had possession of their own WSFS Bank-issued debit cards when the fraudulent transactions were made. WSFS records reflect that before September 13, 2016, each WSFS customer had legitimately used their debit card to purchase gasoline from a common place of business: Sainath Food & Fuel, 820 S. College Avenue, Newark, Delaware.

10. In total, WSFS Bank records reflect that 94 WSFS customers with debit card accounts made legitimate purchases at the Sainath Food & Fuel. Thereafter 265 fraudulent debit card transactions were made against those 94 debit card accounts.

11. In my review of those 265 WSFS transactions, I discovered three transactions involved the purchase of five USPS money orders. I obtained copies of those five USPS money orders and discovered that they were negotiated (*i.e.*, cashed).

12. I also discovered that two of the five money orders were made payable to “Roman Gridjusko” of 9843 Wistaria Street, Philadelphia, Pennsylvania and deposited into GRIDJUSKO's Wells Fargo Bank account. In other words, USPS money orders were deposited into GRIDJUSKO's Wells Fargo account which had been purchased fraudulently using stolen debit/bank card information and PINs from customers of WSFS Bank.

13. In response to WSFS's customer complaints, on September 15, 2016, law enforcement recovered a credit card “skimming device” from the Sainath Food & Fuel. Law enforcement found the skimming device internally interfaced with a gasoline-pump card reader at the business. Through my training, experience, and discussions with other criminal investigators, a skimmer with that design is capable of capturing the name, account number, and PIN of an unsuspecting customer who had used his or her debit card at that pump to purchase gasoline.

III. In November 2016, Gridjusko visited the Friendly Food Mart in Wyomissing, Pennsylvania where a keypad on a gas station was removed

14. Rental records demonstrate GRIDJUSKO rented a white Ford Transit Wagon from between November 17–19, 2016.

15. On November 18, 2016, Fuel Pump #5 at the Friendly Food Mart, 1000 Park Road North, Wyomissing, Pennsylvania, became inoperable. In an effort to prevent customers from using that pump, the owner of Friendly Food Mart placed a trash can in front of the pump until it could be repaired. As confirmed by video surveillance, later that day a white Ford Transit Wagon parked in the fueling area just beyond the trash can in front of Fuel Pump #5. The driver

exited the vehicle and entered the store, and three passengers exited the vehicle and meandered in front of the pump. The three passengers did not purchase gasoline for the vehicle.

16. Based on the video surveillance, the owner of the Friendly Food Mart believes the keypad for Fuel Pump #5 was removed while the white Ford Transit Wagon was parked at the store.

17. The owner interacted with the driver who entered the store. According to the owner, the driver spoke with an "Eastern European accent." GRIDJUSKO is a citizen of Estonia, which is in Eastern Europe.

18. I reviewed the surveillance photo taken that day from inside the store, which captured the driver of the white Ford Transit Wagon. I believe that the driver was GRIDJUSKO based on that image² and the vehicle rental records.

IV. In November 2016, Gridjusko withdrew money from Wawa ATMs by accessing four Diamond Federal Credit Union accounts without authorization whose account information was likely stolen/skimmed at the Friendly Food Mart in Wyomissing, Pennsylvania

19. On November 22, 2017, investigators from the Wyomissing (PA) Police Department initiated an investigation into the fraudulent compromise debit/bank card information.

20. Discussions with bank personnel and a review of bank records revealed that before November 18, 2016, approximately 65 individuals with debit card accounts maintained at multiple banks had used their bank-issued debit cards to legitimately purchase gasoline from a common place of business: Friendly Food Mart, 1000 N. Park Road, Wyomissing, Pennsylvania.

21. According to bank records, after these 65 individuals visited the Friendly Food Mart, fraudulent transactions occurred on their respective debit card accounts, via either (1) unauthorized/fraudulent withdrawals (or attempted withdrawals) of cash from various ATMs using PINs, or (2) unauthorized/fraudulent purchases of money orders (using PINs) from various convenience stores and USPS locations in southeastern Pennsylvania and elsewhere. Most, if not all, of the cardholders still had possession of their own bank-issued debit cards when the fraudulent transactions were made.

22. A review of bank records, including fraud reports, revealed approximately 165 fraudulent transactions were conducted on the 65 separate bank accounts, with an approximate reported loss of \$62,713.29.

23. Of the 65 customer bank accounts who had common transactions at the Friendly Food Mart, four customers of Diamond Federal Credit Union, M.M., K.C., A.L., and C.G.,

² In the course of this investigation I have become familiar with GRIDJUSKO's image, including by attending multiple court hearings where he was present and reviewing his passport photo and other photos. Accordingly, I am familiar with GRIDJUSKO's face, hair, build, and clothing style in mid-to-late 2016.

identified unauthorized/fraudulent transactions that had occurred against each of their respective accounts from between November 21–23, 2016. These included eight unauthorized/fraudulent ATM cash withdrawals totaling \$3,600, which could not have been completed without the use of an access device containing debit/bank card information and a corresponding PIN. These eight ATM transactions occurred at two different Wawa stores near West Chester, Pennsylvania:

Date	Time	Store	Address	City	State	Amount	Name	Last 4
11/21/16	10:50 AM	Wawa #8068	1050 West Chester Pike	West Chester	PA	\$500	M.M.	3018
11/21/16	10:51 AM	Wawa #8068	1050 West Chester Pike	West Chester	PA	\$300	M.M.	3018
11/22/16	11:11 AM	Wawa #25	2 E Rhoads Avenue	West Chester	PA	\$300	K.C.	6001
11/22/16	11:11 AM	Wawa #25	2 E Rhoads Avenue	West Chester	PA	\$500	K.C.	6001
11/23/16	9:54 AM	Wawa #8068	1050 West Chester Pike	West Chester	PA	\$500	A.L.	1005
11/23/16	9:54 AM	Wawa #8068	1050 West Chester Pike	West Chester	PA	\$500	A.L.	1005
11/23/16	9:56 AM	Wawa #8068	1050 West Chester Pike	West Chester	PA	\$500	C.G.	2015
11/23/16	9:56 AM	Wawa #8068	1050 West Chester Pike	West Chester	PA	\$500	C.G.	2015

24. I reviewed Wawa's video surveillance for these two stores for these eight transactions. I believe the person depicted in the video is GRIDJUSKO.

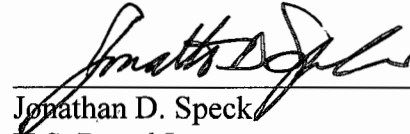
V. Money orders were deposited into Gridjusko's Wells Fargo account which were purchased using skimmed debit/bank card information and PINs without authorization

25. An analysis of GRIDJUSKO's Wells Fargo bank records reveals that at least 43 USPS money orders, totaling \$29,300, were deposited into GRIDJUSKO's Wells Fargo checking account via ATM from between September through November 2016. "Roman Gridjusko," appears as the "payee" on all 43 of the USPS money orders. Most of the money orders have an address of 9843 Wistaria Street, Philadelphia, Pennsylvania.

26. I was able to compare bank records of victims, who had unauthorized/fraudulent transactions on their respective bank accounts, with USPS records and Wells Fargo records. According to that analysis, of the 43 money orders deposited into GRIDJUSKO's Wells Fargo checking account via ATMs, at least 38 of the deposited money orders were purchased using stolen debit/bank card account numbers and PINs.

VI. In December 2016, Berks County Pennsylvania filed state fraud charges against Gridjusko and shortly thereafter he left the U.S.

affidavit does not set forth every fact learned by me or other agents in the course of this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that GRIDJUSKO committed the crimes described herein.


Jonathan D. Speck
U.S. Postal Inspector
U.S. Postal Inspection Service

Sworn and subscribed before me

on July 10, 2017,

BY THE COURT:


HON. DAVID R. STRAWBRIDGE
United States Magistrate Judge